

United States District Court  
For the Northern District of California

Redacted  
Public

**FILED**  
MAY 9 - 2014  
RICHARD W. WIEKING  
CLERK, U.S. DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN JOSE

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN JOSE DIVISION

**14 70655**

**PSG**

In re: [REDACTED]@gmail.com


Case No.

**ORDER DENYING APPLICATION  
FOR A SEARCH WARRANT**

On most days, the undersigned joins the teeming masses of the Bay Area on Highway 101 or 280. Lengthy queues form at each exit in Mountain View, Sunnyvale and Cupertino. Double decker buses pulse with their Wi-Fi as they move past in the diamond lane. On other days, on the ride to the courthouse on Caltrain, passenger after passenger bears the access badges that similarly mark the proliferation of the technology worker. A similar scene plays out as much at the humble downtown San Jose taqueria as the overpriced Palo Alto cafe. The Technorati are, in short, everywhere. And yet too few understand, or even suspect, the essential role played by many of these workers and their employers in facilitating most government access to private citizen's data.

Search warrant applications like the one presently before the court bring this role into view.

Case No.  
**ORDER DENYING APPLICATION FOR SEARCH WARRANT**

DOCUMENT NO.	CSA#
INITIALS	
	
DISTRICT COURT CRIMINAL CASE PROCESSING	

The tools of modern crime have evolved beyond a ski mask and a burlap sack. Like the rest of society, the modern criminal uses computers and mobile devices to do his "work." As such, evidence of crime and evidence of daily life unrelated to crime are often intertwined in software files, folders and databases. Even with a warrant issued under Fed. R. Crim. P. 41, this often leaves the government in the unenviable position of having to spend many, many hours of sifting through data by brute force or complex and cumbersome sorting algorithms. Where the computers at issue are at a suspect's home, courts have recognized the impracticality of reviewing the data on site by approving a "seize first, search second" methodology.<sup>1</sup>

But what about those computers that are not at a suspect's home, but at a third-party cloud provider like Google? Following a standard format used by the Department of Justice, the government draws no distinction and commonly seeks approval for the same seize first, search second methodology whether the data of interest is local or remote. For example, the supporting affidavit here is divided into three sections in which the first section gives background and the reasons sufficient to establish probable cause. In a second section, labeled "Attachment A," the property to be searched is identified as a particular email account stored on the premises of Google's headquarters. No date restriction is included. The third section, labeled "Attachment B," includes two subsections. Subsection I describes particular information within the account to be

<sup>1</sup> See *United States v. Hill*, 459 F.3d 966, 974-75 (9th Cir. 2005) ("[T]he process of searching the files at the scene can take a long time. To be certain that the medium in question does not contain any seizable material, the officers would have to examine every one of what may be thousands of files on a disk-a process that could take many hours and perhaps days. Taking that much time to conduct the search would not only impose a significant and unjustified burden on police resources, it would also make the search more intrusive. Police would have to be present on the suspect's premises while the search was in progress, and this would necessarily interfere with the suspect's access to his home or business. If the search took hours or days, the intrusion would continue for that entire period, compromising the Fourth Amendment value of making police searches as brief and non-intrusive as possible."); see also *United States v. Giberson*, 527 F.3d 882, 887 (9th Cir. 2008) ("[W]here there was ample evidence that the documents authorized in the warrant could be found on a person's computer, the officers did not exceed the scope of the warrant when they seized the computer.").

disclosed by Google.<sup>2</sup> Subsection II describes information from within Subsection I which the government may then seize.<sup>3</sup> As it often does, the government requests delayed notification of the warrant to the account holder, pursuant to 18 U.S.C. § 3103a.<sup>4</sup>

Three elements of the government's application warrant discussion.

First, this application and others like it highlight the problem of devising ex ante limits on the execution of a warrant like those set out in Attachment B. In this ex ante, and also ex parte process, magistrate judges are called on to review the reasonableness of execution procedures like seize first, search second in the sterile isolation of their chambers. All that is available for review

<sup>2</sup> "Information to be disclosed by Google, Inc. (the 'Provider') To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A: (a) The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail; (b) All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number); (c) The types of service utilized; (d) All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; (e) All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken."

<sup>3</sup> "Information to be seized by the government: All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. § 666 (relating to federal program fraud and bribery), 18 U.S.C. § 641 (theft of government property), 18 U.S.C. § 1343 (relating to wire fraud), 18 U.S.C. § 1001 (relating to false statements), and/or 18 U.S.C. § 371 (relating to conspiracy), those violations involving [redacted] and occurring after [redacted], including, for each account or identifier listed on Attachment A, information pertaining to the following matters: (a) Hotel reservations and inquiries; maintenance, housekeeping and customer service requests; hiring, staffing and other employment matters; construction, repair and inspection of the facility; financial management of the [redacted]; use and disbursement of Section 1602 funds; rental contracts, agreements or leases related to the [redacted]; agreements or discussions with the [redacted]; communications between [redacted] and [redacted] related to the use of Section 1602 funds. (b) Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts."

<sup>4</sup> At <https://www.youtube.com/watch?v=MeKKHxcJfh0>, Google provides a very clever stop-animation description of how it says it typically responds.

comes from the government. No defendant or defense counsel is present. Indeed, no defendant yet exists, as no case has yet been filed. There are no hearings, no witnesses, no briefs and no debate. Instead, a magistrate judge is left to predict what would or would not be reasonable in executing the warrant without any hard, ripe facts. This is hardly a recipe for success.<sup>5</sup>

And yet, despite Rule 41(d)(1)'s mandatory language,<sup>6</sup> this court must respect that this Circuit, the Ninth Circuit, has explicitly approved ex ante restrictions in search warrants. In particular, in *United States v. Hill*, the court mandated that agents looking to seize and then search must secure a magistrate judge's approval of the reasonableness of the approach in advance:

Although computer technology may in theory justify blanket seizures for the reasons discussed above, the government must still demonstrate to the magistrate factually why such a broad search and seizure authority is reasonable in the case at hand. There may well be situations where the government has no basis for believing that a computer search would involve the kind of technological problems that would make an immediate onsite search and selective removal of relevant evidence impracticable. Thus, there must be some threshold showing before the government may "seize the haystack to look for the needle."<sup>7</sup>

And so this court must fulfill its duty to consider whether the restrictions of Attachment B pass muster.

This brings the court to the second element worthy of discussion: the constitutionality of the warrant application. As an initial matter, in many ways, the application is remarkably unremarkable. As it does on most days in this court, the government seeks data in the files of an electronic communications service provider as part of an ongoing investigation. Because this same type of request is regularly made in this district, the particular details of the investigation at issue

<sup>5</sup> See *Warshak v. United States*, 532 F.3d 521, 528 (6th Cir. 2008) ("The Fourth Amendment is designed to account for an unpredictable and limitless range of factual circumstances, and accordingly it generally should be applied after those circumstances unfold, not before."); see also Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1278-84 (2010).

<sup>6</sup> "[A] magistrate . . . must issue the warrant if there is probable cause."

<sup>7</sup> 459 F.3d 966, 975 (9th Cir. 2006).

1 here are not important for purposes of this discussion. Suffice it to say that the court finds probable  
2 cause to believe that the Gmail account at issue holds evidence of the theft of government funds.

3 But what of all the data associated with the account which supplies no such evidence  
4 whatsoever? In the Ninth Circuit anyway, the problem is not with seize first, search second itself.  
5 To understand why, go back to *Hill*. *Hill* was undeniably not a third-party provider case; Mr. Hill  
6 possessed all the hardware at issue. But in evaluating the warrant authorizing the seizure and  
7 search of Hill's computers, the Ninth Circuit weighed burdens and practical considerations that, if  
8 anything, are more compelling in a cloud computing environment, not less. Take, for example, the  
9 court's concern with facilitating technical accuracy in searching for the data of interest. In the  
10 absence of a seize first, search second approach, presumably Google (or a special master retained  
11 by Google) would have to search the account at issue looking for just the evidence to be seized.  
12 But even with its search prowess, Google would be left to guess what search terms would be  
13 appropriate. Would it be enough to look for "theft" within five words of "government funds"?  
14 Can Google rely on its famous search engine, or is human review required? Is it reasonable to  
15 impose the cost and, equally important, the distraction of such efforts on a third party to the  
16 investigation, especially in light of the number of times a company like Google gets such a request  
17 every month?  
18

19  
20 Alternatively, consider *Hill*'s concern with the burden on the suspect. Is the suspect better  
21 off with a private firm like Google so intimately involved in a live criminal investigation—or  
22 worse? While Google has publicly declared that it challenges overbroad warrants, in three-plus  
23 years on the bench in the federal courthouse serving its headquarters, the undersigned has yet to see  
24 any such motion. In addition, while not a Ninth Circuit decision, in *United States v. Bach*,<sup>8</sup> the  
25

26  
27  
28 <sup>8</sup> 310 F.3d 1063, 1066-67 (8th Cir. 2002).

1 Eighth Circuit held that the Fourth Amendment permitted essentially the same two-step performed  
2 by Yahoo! at the behest of government investigators. Other district courts have similarly so held.<sup>9</sup>

3 The court is nevertheless unpersuaded that the particular seize first, search second proposed  
4 here is reasonable in the Fourth Amendment sense of the word. On past occasions, the government  
5 at least submitted a date restriction. Here, there is no date restriction of any kind. The activity  
6 described in the application began in 2010; Gmail has been broadly available since 2007 and in  
7 beta release since 2004. Nor has the government made any kind of commitment to return or  
8 destroy evidence that is not relevant to its investigation.<sup>10</sup> This unrestricted right to retain and use  
9 every bit Google coughs up undermines the entire effort the application otherwise makes to limit  
10 the obvious impact under the plain view doctrine of providing such unfettered government access.  
11

12 A final point. This is not the first time that the substance of this application has been before  
13 a magistrate judge. On March 26, 2014, United States Magistrate Judge John Facciola denied a  
14 previous application for a similar warrant in the United States District Court for the District of  
15 Columbia. In his order Judge Facciola cited the “reasons stated in *In re Matter of the Search of*  
16 *Information Associated with [REDACTED]@Mac.com That is Stored at Premises Controlled by*  
17 *Apple, Inc.*, Mag. Case No. 14-228, 2014 WL 945563 (D.D.C. Mar. 7, 2014).” To the  
18 government’s credit, it did not in any way hide its previous unsuccessful effort; in fact it both  
19 provided the disclosure in the sworn affidavit itself and attached a copy of the opinion to the  
20 application materials. And nothing in Rule 41 specifically prohibits this type of follow-up request  
21 in a second district after denial of an application in the first. But there is a long-recognized  
22  
23

24  
25 <sup>9</sup> See, e.g., *United States v. Taylor*, 764 F. Supp. 2d 230, 237 (D. Me. 2011); *United States v.*  
26 *Bickle*, Case No. 10-cr-00565, 2011 WL 3798225, at \*20 (D.Nev. Jul. 21, 2011); *United States v.*  
*Bowen*, 689 F. Supp. 2d 675, 682 (S.D.N.Y. 2010).

27 <sup>10</sup> Cf. *In the Matter of the Search of Information Associated with [Redacted] That is Stored at*  
28 *Premises Controlled by Yahoo! Inc.*, 13 M.J. 728, [#4] (D.D.C. Sept. 25, 2013) (sealed) (Facciola, M.J.).



1 presumption against duplicating court efforts—what some charitably call judge shopping.<sup>11</sup> Even  
2 if a denial of an application were non-appealable,<sup>12</sup> the obvious alternative recourse available to  
3 the government was to seek a writ of mandamus under the All Writs Act or to return to Judge  
4 Facciola with a modified request. Under such circumstances, it would appear that what the  
5 government has chosen to do instead is nothing less than come west looking for a better result.

6 The application is DENIED. The clerk shall file a redacted copy of this order on the public  
7 docket but seal the search warrant, all documents related to search warrant and an unredacted copy  
8 of this order.

9 **IT IS SO ORDERED.**

10 Dated: May 8, 2014

11  
12   
13 PAUL S. GREWAL  
14 United States Magistrate Judge  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

25 <sup>11</sup> See, e.g., *United States v. Leon*, 468 U.S. 897, 918 (1984); *United States v. Richardson*,  
26 943 F.2d 547,551 (5th Cir. 1991); *United States v. Karathanos*, 531 F.2d 26, 34 (2d Cir. 1976).

27 <sup>12</sup> See, e.g. *United States v. Savides*, 658 F. Supp. 1399, 1404 (N.D. Ill. 1987), aff'd sub nom.  
28 *United States v. Pace*, 898 F.2d 1218 (7th Cir. 1990); but see *In re Historical Cellsite Data*,  
724 F.3d 600, 605 (5th Cir. 2013) (collecting cases).